Attorney's Docket No. KAK-0017

ENGLISH LANGUAGE TRANSLATION OF THE ANNEXES TO THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT UNDER PCT ARTICLE 36

Amended Specification and Claims under PCT Article 34

International Application No. PCT/JP2004/016589

Applicants: Masakazu Soga and Toshimitsu Inomata

Title: SECURE PROCESSOR

Rader, Fishman & Grauer PLLC

The objective of the present invention is to provide a processor having general purpose functions and security functions (i.e., safe keeping of key data and high-speed digital signature calculation).

MEASURE TO SOLVE THE PROBLEM

To attain the objective described above, the present invention is a secure processor including: a key register including non-volatile memory stored with key data; a key counter configured to indicate a bit position of the key data stored in the key register to access the key data bit by bit; a digest register configured to be stored with digest data to be used for digital signature; and a gate configured to output 1 for the content of the digest register when the corresponding bit of the key data accessed by the key counter is 0 and output the content of the digest register as is when the bit of the key data is 1; wherein no path for reading all data out from the outside is prepared for the key register, and the secure processor further comprises a plurality of signature dedicated instructions for controlling the key register, the key counter, and the digest register to obtain a digital signature based on the digest data, as well as general instructions.

This allows provision of a processor having a security function, which prohibits key data stored in the key register of non-volatile memory from being read directly, as well as a general function.

Running modes of this processor include a general mode and a security mode. The processor includes a security register configured to indicate the security mode and has a general instruction for setting the security mode and a signature dedicated instruction for resetting the same. The general instruction is effective during the general mode while the signature dedicated instruction is effective during the security mode.

The instruction for setting the security mode causes to set the security register and initializes the key counter to 1023 at the same time while the signature dedicated instruction causes to decrease the key counter by one at the same time when an instruction for conducting signature calculation for one bit of the key register and causes to reset the security mode only when the key counter is 0 resulting from the signature calculation progressing bit by bit. This makes it impossible to leave a digital signature calculation process until the process is completed (i.e., until the key counter becomes 0) once having entered the digital signature calculation process.

Therefore, it is impossible to estimate key data from intermediary results of the calculation using a program.

A means for detecting that each 16 bits of digest data stored in the digest register includes at least one '1' may be provided. The instruction for setting the security mode may cause to initialize the key counter when at least one '1' is included in each 16 bits,

CLAIMS

1. A secure processor, comprising:

a key register including non-volatile memory stored with key data;

a key counter configured to indicate a bit position of the key data stored in the key register to access the key data bit by bit;

a digest register configured to be stored with digest data to be used for digital signature; and

a gate configured to output 1 for the content of the digest register when the corresponding bit of the key data accessed by the key counter is 0 and output the content of the digest register as is when the bit of the key data is 1;

wherein no path for reading all data out from the outside is prepared for the key register, and the secure processor further comprises a plurality of signature dedicated instructions for controlling the key register, the key counter, and the digest register to obtain a digital signature based on the digest data, as well as general instructions.

2. The secure processor according to Claim 1, further comprising:

a general mode and a security mode as processor running modes;

a security register configured to indicate the security mode; and

a general instruction for setting a security mode and a signature dedicated instruction for resetting the same; wherein

the general instruction is effective during the general mode while the signature dedicated instruction is effective during the security mode.

3. The secure processor according to Claim 2, wherein

the instruction for setting the security mode causes to set the security register and initializes the key counter to 1023 at the same time; and

the signature dedicated instruction causes to decrease the key counter by one at the same time when an instruction for conducting signature calculation for one bit of the key register, and causes to reset the security mode only when the key counter is 0 resulting from the signature calculation progressing bit by bit.

4. The secure processor according to Claim 3, further comprising a means for detecting that each 16 bits of digest data stored in the digest register includes at least one '1'; wherein the instruction for setting the security mode causes to initialize the key counter when at least one '1' is included in each 16 bits, and causes to prevent change in data in the digest register after the security register is set.

5. The secure processor according to either Claim 3 or 4, wherein the secure processor is connected to main memory; and the signature dedicated instruction causes to store results of digital signature calculation only in a specific area of the main memory and write the results of digital signature calculation over previous calculation results.

6. An IC card including a secure processor according to either of Claims 1 to 5.